

# Sarbanes-Oxley (SOX) Compliance

The Sarbanes-Oxley Act of 2002 (SOX) protects investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. Among the most significant provisions within Sarbanes-Oxley are the criminal and civil penalties that place executive management and the board of directors in the “hot seat.” Specifically, under Section 404 of the Sarbanes-Oxley Act, executives need to certify and demonstrate that they have established and are maintaining an adequate internal control structure and procedures for financial reporting.

## Objectives to Meet Sarbanes-Oxley Compliance

Sarbanes-Oxley requires a new level of corporate governance and accountability. As a result, the vital role security information and event management (SIEM) plays in establishing and maintaining internal controls has never been greater. Companies must institute log monitoring and vulnerability assessments as a critical part of their IT internal control systems.

Both domestic and international publicly-traded companies must comply with Sarbanes-Oxley. If you are a covered entity, you must have methods to maintain audit trails and to log the possible altering of electronic records. Network Intelligence has mapped best practices and reports to help organizations comply with audits under Sarbanes-Oxley Section 404.

To address the requirements of Section 404, Network Intelligence meets the following objectives:

- **Access Control** monitors attempts to access the company’s financial reporting system or the data that feeds the system.
- **Configuration Control** monitors the configuration, policies and software installed on systems covered by Sarbanes-Oxley and all systems with access to that system.
- **Malicious Software** capabilities detect, collect and report malicious activities caused by viruses or other malicious code from a wide variety of sources with centralized analysis.
- **Policy Enforcement** verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- **User Monitoring and Management** creates a complete audit of the activities of non-employees with access to private data and takes steps to minimize the risk from compromised accounts.
- **Environmental and Transmission Security** involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

*(See chart on page two for specific compliance reports generated for each regulation. While Incident Management requires no specific report, that area is audited so maintaining data in a readily assessable format is recommended. Network Intelligence solutions provide those capabilities.)*

To achieve and maintain compliance in those areas, companies must use the following product capabilities with respect to the data collected by the Network Intelligence Log Management solution:

- **Collect, Protect and Store** data in a non-filtered, non-normalized fashion that is preserved in an efficient and protected manner.
- Establish **Baseline** levels of activity for the entire system and network environment to define “normal activity” and detect unusual levels of activity.
- Efficiently generate the summary and detailed **Reports** spanning the data retention periods mandated by Sarbanes-Oxley.
- **Alert** companies to deviations from baseline activities and complex patterns of malicious activity across multiple, disparate devices.
- **Forensic Analysis** of systems correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
- Establish **Incident Management** capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

These functions ensure that the administrative, physical and technical control demanded by Sarbanes-Oxley regulations are maintained. Network Intelligence solutions address all of the technical standards required.

## The Network Intelligence Internet Protocol Database

Using its advanced LogSmart® Internet Protocol Database™ (IPDB) architecture that is deployed in hundreds of enterprises worldwide, Network Intelligence is able to capture All the Data™ from network, security, host, application and storage layers across the enterprise. The LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization — from the IT department, to the security department, to the compliance and risk officers and executive management.

The benefits of the LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively, without any filtering or data normalization
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance

## Compliance Alerts

Network Intelligence provides the ability to automatically generate alerts based on non-compliance with an observed baseline. This means, should a particular control deviate above certain thresholds, an alert can be triggered and action can be taken to maintain compliance.

OBJECTIVE	SOX REPORT TITLE	DESCRIPTION
Access Control	Administrative Access to Financial Systems	This report shows all login and privileged access attempts by "administrator" or "SU" accounts.
Access Control	Computer Account Login Activity	This report lists all local and remote logon activity for for all monitored Windows, Sun Solaris, Red Hat Linux, HP-UX, and AIX Unix systems.
Access Control	Computer Account Status by Account	This report lists all login activity for specific user accounts. The user accounts in question should be listed as run-time parameters, and multiple values can be specified by listing each value in single quotes and separating them by commas.
Access Control	Failed Login Attempts to Financial Systems	This report lists all local and remote failed login attempts to all monitored devices in the "Financial System" device group.
OBJECTIVE	SOX REPORT TITLE	DESCRIPTION
Configuration Control	Operation Change-control Report	This report lists all configuration and policy changes for the Financial Operational infrastructure.
OBJECTIVE	SOX REPORT TITLE	DESCRIPTION
Malicious Code Detection	Malicious Software Activity	This report lists all malicious software activity for all monitored devices.
OBJECTIVE	SOX REPORT TITLE	DESCRIPTION
Policy Enforcement	Control of Collected Evidence	This report lists all changes and object-level access events to all collected evidence. This report requires that all evidence be contained within directories included in a device group called "Rules for Evidence," and that object-level auditing be enabled on these directories.
Policy Enforcement	Control of Human-resources Data	This report lists all changes and object-level access events to the device group "HR." This report requires that all software and human relations data be contained within a device group, and object-level auditing be enabled on the directories containing the human relations data.
Policy Enforcement	Control of Operational Software	This report lists all changes and object-level access events to the device group, "Operational Software". This report requires that all operational software be contained within a device group, and object-level auditing be enabled on the directories containing the operational software and data.
Policy Enforcement	Control of System-audit Data	This report lists all changes and object-level access events to the software and data used to perform system audits. This report requires that the software, source data and result data be contained within a device group, and object-level auditing be enabled on the containing directories.
Policy Enforcement	Control of System-test Data	This report lists all changes and object-level access events to the systems and data used in the testing of operational software security. This report requires that all system test data be contained within a device group, and object-level auditing be enabled on the directories containing the system-test software, source data and test results.
Policy Enforcement	Financial Data Access	This report lists all successful and failed access attempts for all financial data. This report requires that all financial data be contained within a device group, and object-level auditing be enabled on the directories containing the financial data.
Policy Enforcement	Password Changes and Expirations	This report lists all manual and automatic password change and expiration events. This covers Windows, Sun Solaris, Red Hat Linux, HP-UX and AIX operating systems.
Policy Enforcement	Source-code Access	This report lists all changes and object-level access events to the device group "Source Code." This report requires that the source code for all custom software and commercial software customization be contained within a device group, and object-level auditing be enabled on the directories containing the source code.
OBJECTIVE	SOX REPORT TITLE	DESCRIPTION
User Monitoring	Disabled Accounts Report	This report lists all user accounts that have been manually or automatically disabled in the requested time period.
User Monitoring	External Contractors Report	This report lists all changes and object-level access events to the device group, "External Contractor Access." This report requires that all computers, software, source data and result findings be contained within a device group, and object-level auditing be enabled on the directories containing this data.
User Monitoring	User Activity from External Domains	This report details all activities of non-domain authenticated users. All authenticated domains are identified in run-time parameters, and multiple domains can be contained within single quotes and separated by commas.

### About Network Intelligence Corporation

Network Intelligence is the market-proven leader in transforming enterprise-wide data into automated compliance and security information. The Company's LogSmart® Internet Protocol Database™ (IPDB) provides the only architecture proven to efficiently collect and protect All the Data™, from any IP device, without filtering or agents. Network Intelligence takes the cost and complexity out of compliance and security for hundreds of customers worldwide, including five of the *Fortune 10*.